AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated in the following listing of all claims:

1. (Previously presented) A method comprising:
selecting a fixed length segment of a continuous decryption key stream based on a received session count of a received data packet; and
padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and
decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding.

2. (Previously presented) A method in accordance with claim 1, wherein the applying comprises performing a bit per bit stream decryption process.

3. (Original) A method in accordance with claim 2, wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet.

4. (Canceled)

5. (Original) A method in accordance with claim 2, further comprising:
receiving the data packet, the data packet comprising at least a portion of the received session count.

6. (Original) A method in accordance with claim 5, wherein the data packet further comprises at least a portion of a received message digest value.

7. (Original) A method in accordance with claim 5, wherein the selecting comprises:

selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value.

8. (Original) A method in accordance with claim 7, wherein the selecting further comprises:

extracting the at least a portion of the received session count from the encrypted data packet;

expanding the at least a portion of the received session count to the received session count; and

comparing the received session count to the locally generated session count.

9. (Original) A method in accordance with claim 8, further comprising:

discarding the data packet if the difference is not less than the threshold value.

10. (Previously presented) A method in accordance with claim 9, further comprising:

re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference is not less than the threshold value.

11. (Original) A method in accordance with claim 6, further comprising:

discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value.

12. (Original) A method in accordance with claim 11, further comprising:

re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value.

13. (Original) A method in accordance with claim 12, further comprising:

extracting the at least a portion of the received message digest value from the data packet;

generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key;

truncating the locally generated message digest value to form a truncated message digest; and

comparing the truncated message digest to the at least a portion of the received message digest value.

14. (Previously presented) A method of generating an encrypted data packet, the method comprising:

padding data to generate padded data;

selecting a fixed length segment of a continuous encryption key stream;

applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding;

de-padding the padded encrypted data to form the encrypted payload;

generating a session count based in accordance with the fixed length segment; and

combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet.

15. (Original) A method in accordance with claim 14, wherein the applying comprises performing a bit per bit streaming encryption process.

16. (Original) A method in accordance with claim 15, wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet.

17. (Canceled)

18. (Original) A method in accordance with claim 14, further comprising:

generating a message digest value; and

combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet.

19. (Original) A method in accordance with claim 18, wherein the generating comprises:
generating the message digest value based on the encrypted payload, the session count and a message digest key.

20. (Original) A method in accordance with claim 18, further comprising:
forming the at least a portion of the message digest value by truncating the message digest value.

21. (Original) A method in accordance with claim 14, further comprising transmitting the encrypted data packet to a receiver through a communication channel.

22. (Original) A method in accordance with claim 14, further comprising:
receiving a received data packet corresponding to the encrypted data packet,
the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value;
selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and
decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet.

23. – 25. (Canceled)

26. (Previously presented) A method in accordance with claim 22, wherein the selecting the fixed length segment of the continuous decryption key stream comprises:
selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value.

27. (Original) A method in accordance with claim 26, wherein the selecting further comprises:

extracting the at least a portion of the received session count from the received encrypted data packet;

expanding the at least a portion of the received session count to the received session count; and

comparing the received session count to the locally generated session count.

28. (Original) A method in accordance with claim 27, further comprising:

discarding the received encrypted data packet if the difference is not less than the threshold value.

29. (Currently amended) A method in accordance with claim 28, further comprising:

re-synchronizing the decryption key to the encryption key by setting the decryption key and the encryption key to a start vector if the difference [in] is not less than the threshold value.

30. (Original) A method in accordance with claim 26, further comprising:

discarding the received encrypted data packet if the received truncated message digest value does not match a truncated locally generated message digest value.

31. (Original) A method in accordance with claim 30, further comprising:

re-synchronizing the decryption key stream to an encryption key stream by setting the decryption key stream and the encryption key stream to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value.

32. (Original) A method in accordance with claim 31, further comprising:

extracting the received truncated message digest value from the received encrypted data packet;

generating a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key;

truncating the locally generated message digest value to form the locally generated truncated message digest value; and

comparing the locally generated truncated message digest value to the received truncated message digest value.

33.-40. (Canceled)

41. (Previously presented) A transmitter configured to generate an encrypted data packet, the transmitter comprising:

a padding engine configured to generate padded data;

an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data;

a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload; and

a session count generator configured to generate a packet number in accordance with the fixed length segment, the encrypted data packet comprising the encrypted payload and at least a portion of the session count.

42. (Original) A transmitter in accordance with claim 41, wherein the encryption engine is configured to perform a bit per bit streaming encryption process.

43. (Original) A transmitter in accordance with claim 42, wherein the encryption engine is further configured to perform an exclusive OR operation with the portion of the fixed length segment and the data packet.

44. (Canceled)

45. (Original) A transmitter in accordance with claim 42, further comprising:

a message digest generator configured to generate a message digest value, the encrypted data packet comprising at least a portion of the message digest value.

46. (Original) A transmitter in accordance with claim 45, wherein the message digest generator is further configured to generate the message digest value based on the encrypted payload, the session count and a message digest key.

47. (Original) A transmitter in accordance with claim 46, further comprising:

a truncator configured to truncate the message digest value to form the at least a portion of the message digest value.

48.-56. (Canceled)

57. (Currently amended) ~~The receiver of claim 33 further comprising:~~A receiver comprising:

a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold;

a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine; ~~and~~

a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold; and

a pad remover configured to remove padding from the decrypted data.